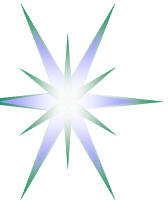
Fonkey Project Update:
Target Applications

TechSec WG, RIPE-45

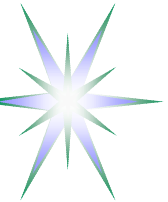
May 14, 2003

Yuri Demchenko <demch@NLnetLabs.nl>



Outline

- Fonkey Project Status
- Design issues
- Target applications



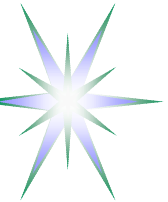
Fonkey Project Status

Fonkey (former Donkey) Project at NLnet Labs - http://www.nlnetlabs.nl/fonkey/

- System to distribute cryptographic keys and reference/attribute information bound by Digital Signature
  - To serve as a sort of identification

Project Status

- Current stage – definition and pilot implementation of basic client-storage functionality, including
  - Package format
  - Simple query language
  - Publish, retrieve, search protocols
  - Demo - available mid June
- For the next stage – p2p network infrastructure and related protocol and data format issues



What is Fonkey: Fonkey functionality

- Fonkey allows anyone to publish a named key, together with optional data (Fonkey package)
  - Fonkey is NOT a permanent storage: key must be republished to remain available
  - Fonkey does NOT define a policy for key/payload usage
    - This is an application specific function
- Fonkey allows anyone to search for a published key, based on the key's name (required) and signers (optional)
- Fonkey allows anyone to sign a published key

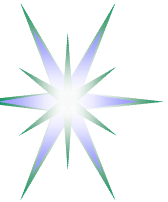
Design issues: Package structure

- **Type –** Type of Package: (Key | Named | Signature)
- **Key –** Owner's public key
- **Properties –** A set of name/value pairs
  - To serve control/status and identification function
- **Payload -** Application specific content and format
  - May include specific format definition (e.g., embedded XML Schema)
- **Signatures –** Signature used to ensure integrity and identity of Package
  - Signed by Owner's private key
  - Signed by others

Design issues: Types of Package

Generic Package structure –
{Type, Public Key, Properties, Payload, Signature}

- **Key Package** – like generic package
  - Unique ID is defined by Public Key
  - Location by Public Key attributes/info
- **Named Package** – adds Name field to the generic package
  - Unique ID is defined by Name and Key
  - Location by Name
- **Signature Package** – adds Subject (ID of the package signed by this Signature) and References (to signed parts/portions)
  - Unique ID is defined by Public Key and Subject
  - Location by (Subject, Public Key) pair



Design issues: More information

Package format

- Currently used Python data object format as an internal format and XML based exchange format
- Prospectively internal XML format and XML Protocol

More information – Fonkey Project Overview

http://www.nlnetlabs.nl/fonkey/donkey-overview.pdf

Fonkey Target Applications

Fonkey is kept as simple as possible to create easily deployable infrastructure

- Analysis of target applications requirements allows to define specific requirements and necessary extensions to the generic/basic functionality

Applications under discussion

- PGP Keyserver with extended payload
- Privilege Storage (bound to PK based identity)
- Identity Server for Liberty Project applications – *under discussion*
- Other applications
  - Location Server for IIDS
  - Client applications requiring XMLSig functionality, e.g. WS/SOAP based AAA Agent, IODEF enabled Incident Handling System

Target Application: Extended PGP Keyserver

Reference - The OpenPGP HTTP Keyserver Protocol (HKP)
http://www.ietf.org/internet-drafts/draft-shaw-openpgp-hkp-00.txt

Specific requirements

- PGP key request via HTTP GET
  - Operations - {get, index, vindex, x-?}
  - Search - variable {key ID, V4 Fingerprint, V3 Fingerprint}
  - Modifier = {options {mr, nm}, fingerprint, exact
- PGP key publish via HTTP POST
  - OpenPGP Packet in an ASCII Armored format (RFC2440)

Benefits/new functionality with Fonkey

- Adding application oriented payload
- Flexible search for Key information
- Building P2P infrastructure
- Integration with other types of PK infrastructures

Target Application: Privilege Storage (for PMI)

Specific Requirements

- Publish and retrieve/search for Subject's Attribute Certificate/Package
- Administrative interface for generating role-based AC (not necessary X.509)

Benefits

- Flexibility in using XML Schema for Subject's attributes comparing to LDAP
- Possibility to integrate with PKC storage

Issues to solve

- Policy definition
- Administrative interface
- Using SAML for attributes assertions

Prospective Target Applications: Identity Server

Prospective Target application – Identity Server for federated identity management with Liberty Alliance Project (LAP)

- New set of LAP specifications published - http://www.projectliberty.org/
  - Using SAML and Web Services technology
  - Trust management for dynamic identity federation
    - Circles of trust initiated and controlled by user

Promising area – needs further discussion

Other possible uses (not intended)

- Applications requiring XML Signature based functionality
  - Adding XML Signature to proprietary XML Documents (e.g., IODEF)
  - Adding XML Signature to SOAP based applications (e.g., AAA/Web Services)
  - Mostly limited to Client functionality
- Location Server for IIDS (Interactive Intelligent Distributed Systems)